CLAIMS

WHAT IS CLAIMED IS:

1. A communications method, comprising operations of:

conducting digitally signed and encrypted synchronous online messages between online messaging service subscribers.

2. The method of claim 1, the messages comprising text content.

3. The method of claim 1, the messages comprising text content and files.

4. The method of claim 1, the conducting operation comprising:

utilizing a messaging server to relay digitally signed and encrypted text messages;

relaying digitally signed and encrypted files independent of the messaging server.

5. The method of claim 1, each subscriber including respective local instant messaging software programmed to exchange unsecured synchronous online messages between prescribed subscribers, the conducting operation comprising:

each subscriber's instance of local instant messaging software utilizing information of one or more digital certificates associated with that subscriber to sign and encrypt outgoing messages, and utilizing information of one or more digital certificates of senders to authenticate and decrypt incoming messages from those senders.

6. The method of claim 1, where:

the subscribers include respective local instant messaging software instances;

the operations further comprise each instance of local instant messaging software importing any digital certificates existing at the respective subscriber for use in signing and encrypting of synchronous online messages.

7. A method of managing the exchange of secure online instant messages between subscriber devices, where the secure messages are signed and encrypted using subscribers' digital certificates, the method comprising operations of:

at one or more subscriber devices, an associated local instant messaging module logging in to a messaging server to begin a session of exchanging synchronous online messages;

at one or more of the logged-in devices, the associated local instant messaging module submitting a certificate publication request to a messaging server, the publication request also specifying a digital certificate corresponding to the subscriber device;

responsive to each certificate publication request, the messaging server temporarily storing the submitted digital certificate in a publication record in association with the submitting device as long as the associated instant messaging module remains logged-in to the messaging server;

responsive to prescribed events, the messaging server providing logged-in subscriber devices with selected information concerning certificates of other subscriber devices.

8. The method of claim 7, the operation of, responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificate status of other subscriber devices comprising:

responsive to a request from one subscriber device to establish a dialog with another subscriber device, the messaging server providing the requesting subscriber device with a representation of a digital certificate of the other subscriber device from the publication record.

9. The method of claim 7, the operation of, responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificate status of other subscriber devices comprising:

responsive to a particular subscriber device's request to publish a new digital certificate, the messaging server identifying other logged-in subscriber devices that have designated the particular subscriber device for potential future secured instant messaging, and providing the identified devices with a representation of the new digital certificate.

10. The method of claim 7, the operation of, responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificate status of other subscriber devices comprising:

receiving a particular subscriber device's request to un-publish its digital certificate;

responsive to receiving the request, the messaging server removing the digital certificate from the publication record, identifying other logged-in subscriber devices that previously designated the particular subscriber device for potential future secured instant messaging, and notifying the identified devices of the digital certificate withdrawn from use.

11. The method of claim 10, further comprising:

the particular subscriber device submitting the request to un-publish its digital certificate in response to at least one of the following events: (1) physical unavailability of the subscriber device's digital certificate, (2) logical unavailability of the subscriber device's corresponding digital certificate, (3) user election to un-publish the subscriber device's digital certificate.

12. The method of claim 7, the operation of, responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificate status of other subscriber devices comprising:

responsive to a request from a first subscriber device to establish a dialog with a second subscriber device, the messaging server denying supplication of the second subscriber's digital certificate to the first subscriber whenever the second subscriber's digital certificate has experienced one or more of the following actions: invalidity, revocation, un-publication.

13. The method of claim 7, further comprising:

delaying submittal of the certificate publication request under preventive circumstances including at least one of the following: (1) physical unavailability of the digital certificate, (2) logical unavailability of the digital certificate, (3) user election to delay publication of the digital certificate.

14. The method of claim 13, further comprising:

automatically submitting the certificate publication request when the preventive circumstances terminate.

15. The method of claim 7, the operation of, responsive to prescribed events, providing logged-in subscriber devices with information concerning certificate status of other subscriber devices comprising:

responsive to a particular subscriber device's published certificate becoming invalid, the messaging server identifying other logged-in subscriber devices that previously designated the particular subscriber device for potential future secured instant messaging, and notifying the identified devices of the invalid digital certificate.

16. The method of claim 7, the operation of temporarily storing the submitted digital certificate additionally storing a representation of a chain record pertaining to the certificate, where storage of repetitive chain records are abbreviated to conserve storage space

17. The method of claim 7, the act of submitting the publication request is performed under one or more of the following conditions: (1) automatically in response to the act of logging in to the messaging server, (2) manually in response to operator direction.

18. The method of claim 7, further comprising operations of:

at one or more of the logged-in devices, an associated local instant messaging module submitting a certificate un-publication request to the messaging server responsive to specified conditions;

responsive to each un-publication request, the messaging server removing the requesting subscriber's digital certificate from the publication record.

19. The method of claim 7, where:

the operations further comprise, responsive to each publication request, the messaging server receiving revocation information for the subscriber's certificate;

upon expiration of the certificate as indicated by the revocation information, removing the subscriber's certificate from the publication record.

20. The method of claim 7, further comprising:

at one or more of the logged-in devices, the associated local instant messaging module obtaining revocation information for the digital certificate corresponding to the subscriber device;

the messaging server temporarily storing the obtained revocation information in the publication record in association with the submitting device as long as the associated instant messaging module remains logged-in to the messaging server.

21. The method of claim 20, the operations further comprising:

the respective local instant messaging module storing the obtained revocation information and, as long as the associated digital certificate is still valid, utilizing the revocation information in future sessions to avoid having to re-obtain the revocation information.

22. The method of claim 7, further comprising operations of:

prior to engaging in secured communications with a first subscriber device, a second subscriber device's local instant messaging module communicating with the messaging server to determine whether the first subscriber device's digital certificate is valid, and if not, refraining from secured synchronous communications with the first subscriber device.

23. A messaging server for use in managing the exchange of secure online instant messages between subscriber devices, where the secure messages are signed and encrypted using subscribers' digital certificates, the messaging server comprising:

storage;

at least one digital data processor coupled to the storage;

the data processor programmed to perform operations comprising:

beginning a session of exchanging synchronous online messages by receiving log-in from local instant messaging modules of one or more subscriber devices;

receiving from one or more of the logged-in devices' associated local instant messaging modules a certificate publication request specifying a digital certificate corresponding to the subscriber device;

responsive to each certificate publication request, temporarily storing the submitted digital certificate in a publication record in association with the submitting device as long as the associated instant messaging module remains logged-in to the messaging server;

responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificates of other subscriber devices.

24. The messaging server of claim 23, the processor programmed such that the operation of, responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificate status of other subscriber devices comprises:

responsive to a request from one subscriber device to establish a dialog with another subscriber device, the messaging server providing the requesting subscriber device with a representation of a digital certificate of the other subscriber device from the publication record.

25. The messaging server of claim 23, the processor programmed such that the operation of, responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificate status of other subscriber devices comprises:

responsive to a particular subscriber device's request to publish a new digital certificate, the messaging server identifying other logged-in subscriber devices that have designated the particular subscriber device for potential future secured instant messaging, and providing the identified devices with a representation of the new digital certificate.

26. The messaging server of claim 23, the processor programmed such that the operation of, responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificate status of other subscriber devices comprises:

receiving a particular subscriber device's request to un-publish its digital certificate;

responsive to receiving the request, removing the digital certificate from the publication record, identifying other logged-in subscriber devices that previously designated the particular subscriber device for potential future secured instant messaging, and notifying the identified devices of the digital certificate withdrawn from use.

27. The messaging server of claim 23, the processor programmed such that the operation of, responsive to prescribed events, providing logged-in subscriber devices with selected information concerning certificate status of other subscriber devices comprises:

responsive to a request from a first subscriber device to establish a dialog with a second subscriber device, server denying supplication of the second subscriber's digital certificate to the first subscriber whenever the second subscriber's digital certificate has experienced one or more of the following actions: invalidity, revocation, un-publication.

28. The messaging server of claim 23, the processor programmed such that the operation of, responsive to prescribed events, providing logged-in subscriber devices with information concerning certificate status of other subscriber devices comprises:

responsive to a particular subscriber device's published certificate becoming invalid, identifying other logged-in subscriber devices that previously designated the particular subscriber device for potential future secured instant messaging, and notifying the identified devices of the invalid digital certificate.

29. The messaging server of claim 23, the processor programmed such that the operation of temporarily storing the submitted digital certificate additionally comprises storing a representation of a chain record pertaining to the certificate, where storage of repetitive chain records are abbreviated to conserve storage space

30. The messaging server of claim 23, the processor additionally programmed to perform operations comprising:

responsive to each logged-in subscriber device's request to un-publish a digital certificate, the messaging server removing the requesting subscriber's digital certificate from the publication record.

31. The messaging server of claim 23, where:

the processor is programmed to perform further operations, comprising, responsive to each publication request, the messaging server receiving revocation information for the subscriber's certificate, and upon expiration of the certificate as indicated by the revocation information, removing the subscriber's certificate from the publication record.

32. A communications method, comprising operations of:

providing an online instant messaging center to serve multiple prescribed subscribers;

providing instant messaging software for installation by the subscribers;

where the center and software are configured to cooperatively exchange digitally signed and encrypted synchronous online messages between groups of two or more dialoging subscribers.

33. The method of claim 32, the center and software are configured such that:

the messages include text content.

34. The method of claim 32, the center and software are configured such that:

the messages include text content and files.

35. The method of claim 32, where:

the messaging center and software are configured to utilize the messaging center to relay digitally signed and encrypted text messages;

the software is configured to relay digitally signed and encrypted files independent of the messaging server.

36. The method of claim 32, where each instance of the software is further configured to import any digital certificates existing at the respective subscriber for use in signing and encrypting of synchronous online messages.

37. An online instant messaging system, comprising:

an online instant messaging center to serve multiple prescribed subscribers;

instant messaging software for installation by the subscribers;

where the center and software are configured to cooperatively exchange digitally signed and encrypted synchronous online messages between groups of two or more dialoging subscribers.

38. An online instant messaging system, comprising:

online instant messaging center means for serving multiple prescribed subscribers;

instant messaging software means for installation by the subscribers;

where the center means and software means are configured to cooperatively exchange digitally signed and encrypted synchronous online messages between groups of two or more dialoging subscribers.